REMARKS

Prior to entry of the present Amendment, claims 1-5, 11-30, 32-57, 59-63, 85-87, 89-92, 98-116, 118-127, 128-133 and 155-157, 159-183 were pending in the present application. Claims 20, 25, 107, 111 and 159 are cancelled above, without prejudice to their being filed in continuation or divisional applications. Claims 1, 24, 29, 51, 56, 85, 115, 126, 155, 161, 167, 175 and 180-183 are amended above. New claims 184-193 are added above. No new matter is added by the new claims and claim amendments. Entry is respectfully requested.

The Applicants note that in Amendment A dated September 21, 2006, claim 1 was amended to incorporate the limitations of then-allowed claim 10 and intervening claims 6-9. Since the current Office Action dated December 8, 2006 indicates that the subject matter of claims 6-10 is no longer allowable, claim 1 is currently amended to remove the limitations of former claims 6-10 from claim 1 and new dependent claims 184-188 are added to include the subject matter of former claims 6-10. In addition, the Applicants note that in the Amendment A dated September 21, 2006, claim 89 was amended to incorporate the limitations of then-allowed claim 97 and intervening claims 93-96. Since the current Office Action dated December 8, 2006 indicates that the subject matter of claims 93-97 is no longer allowable, claim 89 is currently amended to remove the limitations of former claims 93-97 from claim 89 and new dependent claims 189-193 are added to include the subject matter of former claims 93-97.

Claims 24 and 51 stand objected to for reasons discussed in the Office Action. The claims are amended in a manner consistent with suggestions made in the Office Action. Reconsideration of the objections to the claims is respectfully requested.

Claims 1-5, 11-14, 20, 25, 26, 89-92, 98-101, 107, 111 and 112 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* (U.S. Publication Number 2002/0003881) in view of Weidong (U.S. Patent Number 6,819,766). Claims 15-19, 21-24, 102-106 and 108-110 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.*

in view of Wiedong and Jensen, *et al.* (U.S. Patent Number 5,930,828). Claims 27, 28, 113, 114 and 159 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Weidong and Xu, *et al.* (U.S. Publication Number 2006/0053307). The Applicants note that claim 159 is cancelled. Claims 29, 30, 32-39, 43-53, 85-87, 115, 116, 118-121, 123-125, 155-157, 161-166, 180-183 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* Claims 40, 41, 42 and 122 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Weidong. Claims 54 and 55 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Xu, *et al.* Claims 56, 57, 59-63, 126, 127, 129, 130, 132, 133, 167-171, 175 and 176 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* Claims 172-174 and 177-179 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Jensen, *et al.* Claims 131 and 61 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Atallah, *et al.* (U.S. Publication Number 2006/0031686). Reconsideration of the rejection and allowance of the claims are respectfully requested.

In the present invention as claimed in independent claims 1, 161 and 167, a method of preventing unauthorized use of digital content data includes subdividing the digital content data into data segments, modifying the data segments with second data to generate modified data. Modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data. The method further includes storing the modified data at predetermined memory locations. The method further includes retrieving the modified data from the predetermined memory locations and, following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments.

In the present invention as claimed in independent claim 29, a method of preventing unauthorized use of digital content data in a system having memory locations includes subdividing the digital content data into data segments and modifying the data segments with second data to generate modified data. The method further includes scanning the system to determine available memory locations, selecting target memory locations with the available

memory locations at which to store the modified data and storing the modified data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system.

In the present invention as claimed in independent claim 56, a method for preventing unauthorized use of digital content data hosted on a system includes modifying digital content data to generate modified data. The method further includes determining whether an unauthorized attempt at accessing the digital content data occurs and, in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter the unauthorized activity.

In the present invention as claimed in independent claim 85, a method for preventing unauthorized use of digital content data in a system having memory locations includes scanning the system to determine available memory locations, selecting target memory locations within the available memory locations and storing the digital content data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system.

In the present invention as claimed in independent claims 89 and 175, a system for preventing unauthorized use of digital content data includes a subdividing unit for subdividing the digital content data into data segments, a modification unit for modifying the data segments with second data to generate modified data. Modifying the data segments includes interleaving the data segments with the second data to generate interleaved data. The system further includes a storage unit for storing the modified data at predetermined memory locations. The system further includes a means for retrieving the modified data from the predetermined memory locations and a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original digital content data.

In the present invention as claimed in independent claim 115, a system for preventing unauthorized use of digital content data in a system having memory locations includes a means for subdividing the digital content data into data segments and a means for modifying the data segments with second data to generate modified data. The system further includes a means for scanning the system to determine available memory locations, a selector for selecting target memory locations within the available memory locations and a storage unit for storing the modified data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system.

In the present invention as claimed in independent claim 126, a system for preventing unauthorized use of digital content data hosted on a system includes a modification unit for modifying the digital content data to generate modified data. The system further includes a means for determining whether an unauthorized attempt at accessing the digital content data occurs, and, in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter the unauthorized activity.

In the present invention as claimed in independent claim 155, a system for preventing unauthorized use of digital content data in a system having memory locations includes a scanner for scanning the system to determine available memory locations based on a file system identifying locations of files on the system, a means for selecting target memory locations within the available memory locations and a storage unit for storing the digital content data at the target memory locations. A subset of the available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system.

In the present invention as claimed in independent claim 180, a system for preventing unauthorized use of digital content data includes a subdividing unit for subdividing the digital content data into data segments, a modification unit for modifying the data segments with second data to generate modified data and a storage unit for storing the modified data at predetermined memory locations. The system further includes a scanner for scanning the system to determine

available memory locations and a selector for selecting target memory locations within the available memory locations. The storage unit stores the modified data at the target memory locations and a subset of available memory locations are located outside the bounds of the file system locations as identified by a table of contents of the file system.

Reitmeier, *et al.* discloses a pixel domain encoder 105 which optionally imparts a digital watermarking to video information to produce an encoded information stream. Reitmeier, *et al.* further discloses a segmentation module 110 that divides the encoded or un-encoded information stream into a plurality of segments to produce a segmented information stream. The segmented information stream is then transferred to compression module 115A which compresses the segmented information. The compressed information stream is then transferred to a re-sequencing module 130. Re-sequencing module 130 rearranges the compressed information segments according to a predetermined, or pseudo-random, pattern. That is, re-sequencing module 130 shuffles the compressed and segmented information stream to produce a reordered or re-sequenced compressed information stream and an associated index table indicative of the re-sequencing operation performed. The index table includes pointers to the storage location of sequences ordered in their correct presentation sequence. The information stream is then transferred to encryption module 135 which scrambles the information stream. The index table may be distributed using a different medium than the re-ordered information. The re-ordered information may be distributed on a DVD-ROM, while the index table may be downloaded to a receiver/decoder from an on-line server. A second decryption module 160 decrypts the scrambled sequences. A random access module 165 utilizes the index table information to rearrange the de-scrambled sequences. Decrypted information stream segments are retrieved from a local storage module in a correct temporal or sequential order as indicated by the decrypted index table to produce a properly sequenced compressed information stream.

Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes "modifying the data segments with second data to generate modified data", "modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claims 1, 161 and 167.

Instead, in Reitmeier, *et al.*, the segmented information is not modified with "second data". The Reitmeier, *et al.* re-sequencing module 130 merely rearranges the compressed information segments. The Reitmeier, *et al.* re-sequencing module 130 in no way interleaves the data segments with second data. In addition, the Reitmeier, *et al.* pixel domain encoder 105 modifies the data with second data prior to the segmentation of the data. Therefore, the pixel domain encoder 105 of Reitmeier, *et al.* does not modify the segmented data. The index table of Reitmeier, *et al.* is not used to modify the compressed data and is independent from the re-sequenced data. The Reitmeier, *et al.* index table is merely used to store the locations of the re-sequenced data.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, "following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data", as claimed in independent claims 1, 161 and 167. Instead, in Reitmeier, *et al.*, the compressed information is re-ordered as it is retrieved. The index table retrieves that compressed information in the proper order. While the Reitmeier, *et al.* index table is used to re-order the data, the index table is not used to modify the data originally and does not generate the original content data as claimed in claims 1, 161 and 167.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "modifying the data segments with second data to generate modified data", as claimed in claim 29. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; the segmented information is not modified with "second data" as claimed in claim 29. The Reitmeier, *et al.* pixel domain encoder 105 modifies the data with second data prior to the segmentation of the data. Therefore, the pixel domain encoder 105 of Reitmeier, *et al.* does not modify the segmented data. Once the data has been segmented in Reitmeier, *et al.*, the segmented data is not modified with second data. The index table of Reitmeier, *et al.* is not used to modify the compressed data and is independent from the re-sequenced data. The index table is merely used to store the locations of the re-sequenced data.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of file system locations as identified by a table of contents of the file system", as claimed in claim 29. Instead, Reitmeier, *et al.* merely teaches that the re-ordered sequences and the index table can be distributed over different mediums. The index table of Reitmeier, *et al.* is generated by the re-sequencing module 130 to store pointers to the storage locations of the correct sequences. The Reitmeier, *et al.* index table is not a table of contents of the file system. In addition, the Reitmeier, *et al.* index table stores the locations of the data. Therefore, the locations would not be outside the bounds of the file system as identified by a table of contents because the Reitmeier, *et al.* table of contents identifies where the data locations are. There is no teaching or suggestion of the re-ordered sequences being stored "outside the bounds of file system locations as identified by a table of contents of the file system" as claimed in claim 29.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes "determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 56. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; there is no teaching or suggestion in Reitmeier, *et al.* of reading a saturation profile of a system or the generation of saturation traffic as claimed in claim 56.

In addition, Reitmeier, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 85. Instead, Reitmeier, *et al.* merely teaches that the re-ordered sequences and the index table can be distributed over different mediums. The index table of Reitmeier, *et al.* is generated by the re-sequencing module 130 to store pointers to the storage locations of the correct sequences.

The Reitmeier, *et al.* index table is not a table of contents of the file system. In addition, the Reitmeier, *et al.* index table stores the locations of the data. Therefore, the Reitmeier, *et al.* locations would not be outside the bounds of the file system as identified by a table of contents because the Reitmeier, *et al.* table of contents identifies where the data locations are. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored "outside the bounds of file system locations as identified by a table of contents of the file system" as claimed in claim 85.

Further, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a modification unit for modifying the data segments with second data to generate modified data", the "modification unit modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claims 89 and 175. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; the segmented information is not modified with "second data" as claimed in claims 89 and 175. In Reitmeier, *et al.*, the segmented information is not modified with "second data". The Reitmeier, *et al.* re-sequencing module 130 merely rearranges the compressed information segments. The Reitmeier, *et al.* re-sequencing module 130 in no way interleaves the data segments with second data. In addition, the pixel domain encoder 105 of Reitmeier, *et al.* encodes the data with second data prior to the segmentation of the data. Therefore, the Reitmeier, *et al.* pixel domain encoder 105 does not modify the segmented data. The index table of Reitmeier, *et al.* is not used to modify the compressed data and is independent from the re-sequenced data. The Reitmeier, *et al.* index table is merely used to store the locations of the re-sequenced data.

In addition, Reitmeier, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, "following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data", as claimed in independent claims 89 and 175. Instead, in Reitmeier, *et al.*, the compressed information is re-ordered as it is retrieved. The Reitmeier, *et al.* index table retrieves that compressed information in the proper order. While the Reitmeier, *et al.* index table

is used to re-order the data, the Reitmeier, *et al.* index table is not used to modify the data originally and does not generate the original content data as claimed in claims 89 and 175.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes a "means for modifying the data segments with second data segments to generate modified data", as claimed in independent claim 115. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; the segmented information is not modified with "second data" as claimed in claim 115. The Reitmeier, *et al.* pixel domain encoder 105 modifies the data with second data prior to the segmentation of the data. Therefore, the pixel domain encoder 105 of Reitmeier, *et al.* does not modify the segmented data as claimed in claim 115. Once the data has been segmented in Reitmeier, *et al.*, the segmented data is not modified with second data. The index table of Reitmeier, *et al.* is not used to modify the compressed data and is independent from the re-sequenced data. The Reitmeier, *et al.* index table is merely used to store the locations of the re-sequenced data.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of the available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents", as claimed in independent claim 115. Instead, Reitmeier, *et al.* merely teaches that the re-ordered sequences and the index table can be distributed over different mediums. The index table of Reitmeier, *et al.* is generated by the re-sequencing module 130 to store pointers to the storage locations of the correct sequences. The Reitmeier, *et al.* index table is not a table of contents of the file system. In addition, the Reitmeier, *et al.* index table stores the locations of the data. Therefore, the Reitmeier, *et al.* locations would not be outside the bounds of the file system as identified by a table of contents because the Reitmeier, *et al.* table of contents identifies where the data locations are. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored "outside the bounds of file system locations as identified by a table of contents of the file system" as claimed in claim 115.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a "means for determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 126. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; there is no teaching or suggestion in Reitmeier, *et al.* of the reading of a saturation profile of a system or the generation of saturation traffic as claimed in claim 126.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 155. Instead, Reitmeier, *et al.* merely teaches that the re-ordered sequences and the index table can be distributed over different mediums. The index table of Reitmeier, *et al.* is generated by the re-sequencing module 130 to store pointers to the storage locations of the correct sequences. The Reitmeier, *et al.* index table is not a table of contents of the file system. In addition, the Reitmeier, *et al.* index table stores the locations of the data. Therefore, the Reitmeier, *et al.* locations would not be outside the bounds of the file system as identified by a table of contents because the Reitmeier, *et al.* table of contents identifies where the data locations are. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored "outside the bounds of file system locations as identified by a table of contents of the file system" as claimed in claim 155.

Further, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a "modification unit for modifying the data segments with second data to generate modified data", as claimed in independent claim 180. Instead, in Reitmeier, *et al.*, the segmented information is either compressed, rearranged or scrambled; the segmented information is not modified with "second data" as claimed in claim 180. The

Reitmeier, *et al.* pixel domain encoder 105 modifies the data with second data prior to the segmentation of the data. Therefore, the pixel domain encoder 105 of Reitmeier, *et al.* does not modify the segmented data. Once the data has been segmented in Reitmeier, *et al.*, the segmented data is not modified with second data as claimed in claim 180. The index table of Reitmeier, *et al.* is not used to modify the compressed data and is independent from the re-sequenced data. The Reitmeier, *et al.* index table is merely used to store the locations of the re-sequenced data.

In addition, Reitmeier, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a "subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent 180. Instead, Reitmeier, *et al.* merely teaches that the re-ordered sequences and the index table can be distributed over different mediums. The index table of Reitmeier, *et al.* is generated by the re-sequencing module 130 to store pointers to the storage locations of the correct sequences. The Reitmeier, *et al.* index table is not a table of contents of the file system. In addition, the Reitmeier, *et al.* index table stores the locations of the data. Therefore, the Reitmeier, *et al.* locations would not be outside the bounds of the file system as identified by a table of contents because the Reitmeier, *et al.* table of contents identifies where the data locations are. There is no teaching or suggestion of the Reitmeier, *et al.* re-ordered sequences being stored "outside the bounds of file system locations as identified by a table of contents of the file system" as claimed in claim 180.

Weidong appears to disclose a method for managing encryption keys for data that includes generating a session key, encrypting the data using the session key and generating a key encryption key based on an initial vector. The initial vector is known only to a party encrypting the data and a party intended to decrypt the data. The session key is encrypted using the key encryption key.

Like Reitmeier, *et al.*, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data that includes "modifying the data segments with second data to generate modified data", "modifying the data segments" comprising "interleaving the data

segments with the second data to generate interleaved data", as claimed in independent claim 1. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "modifying the data segments" with second data as claimed in claim 1. In addition, like Reitmeier, *et al.*, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, "following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data", as claimed in independent claim 1. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "de-interleaving the data segments based on the second data" as claimed in claim 1.

Further, like Reitmeier, *et al.*, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "modifying the data segments with second data to generate modified data", as claimed in claim 29. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "modifying the data segments" with second data as claimed in claim 29. In addition, Weidong fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of file system locations as identified by a table of contents of the file system", as claimed in claim 29.

In addition, like Reitmeier, *et al.*, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a modification unit for modifying the data segments with second data to generate modified data", the "modification unit modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claim 89. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "modifying the data segments" with second data. In addition, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data", as claimed in independent claim 89. Weidong in no

way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "de-interleaving the data segments based on the second data" as claimed in claim 89.

In addition, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes a "means for modifying the data segments with second data segments to generate modified data", as claimed in independent claim 115. Weidong in no way teaches or suggest segmenting the data, and, therefore, fails to teach or suggest "modifying the data segments" with second data as claimed in claim 115. In addition, Weidong fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of the available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 115.

Jensen, *et al.* is cited in the Office Action as teaching scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data. Jensen, *et al.* appears to disclose that information regarding locations of files is contained in a master file table.

Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes "modifying the data segments with second data to generate modified data", "modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claims 1, 161 and 167. In addition, Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, "following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data", as claimed in independent claims 1, 161 and 167.

Jensen, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "modifying the data segments with second data to generate modified data", as claimed in claim 29. In addition, Jensen, *et al.*

fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of file system locations as identified by a table of contents of the file system", as claimed in claim 29. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 85. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a modification unit for modifying the data segments with second data to generate modified data", the "modification unit modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claims 89 and 175. In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data", as claimed in independent claims 89 and 175.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes a "means for modifying the data segments with second data segments to generate modified data", as claimed in independent claim 115. In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes "a

subset of the available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 115. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

Further, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 155. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a "modification unit for modifying the digital content data to generate modified data", as claimed in independent claim 180. In addition, Jensen, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes a "subset of available memory locations" that "are located outside the bounds of the file system locations as identified by a table of contents of the file system", as claimed in independent claim 180. Rather, in Jensen, *et al.*, the information regarding locations of files is contained in a master file table, and, therefore, the files are located within the bounds of the file system as identified by the master file table.

Xu, *et al.* appears to disclose using obfuscation to prevent accurate disassembly of computer code. Assembly language instructions are used to confuse a disassembler.

Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes "modifying the data segments with second data to generate modified data", "modifying the data segments" comprising "interleaving the data segments with the second

data to generate interleaved data", as claimed in independent claims 1 and 167. In addition, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data that includes, "following retrieving the modified data, de-interleaving the data segments based on the second data used to modify the data segments to generate original digital content data", as claimed in independent claims 1 and 167.

Further, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "modifying the data segments with second data to generate modified data", as claimed in claim 29. In addition, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data in a system having memory locations that includes "a subset of available memory locations" that "are located outside the bounds of file system locations as identified by a table of contents of the file system", as claimed in claim 29.

In addition, like Reitmeier, *et al.*, Xu, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes "determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 56.

In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a modification unit for modifying the data segments with second data to generate modified data", the "modification unit modifying the data segments" comprising "interleaving the data segments with the second data to generate interleaved data", as claimed in independent claims 89 and 175. In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data that includes "a means for de-interleaving the data segments, following retrieving the modified data, based on the second data used to modify the data segments to generate original data", as claimed in independent claims 89 and 175.

In addition, Xu, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a "means for determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 126.

Atallah, *et al.* is cited in the Office Action as disclosing that determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted.

Atallah, *et al.* fails to teach or suggest a method of preventing unauthorized use of digital content data hosted on a system that includes "determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 56.

In addition, Atallah, *et al.* fails to teach or suggest a system for preventing unauthorized use of digital content data hosted on a system that includes a "means for determining whether an unauthorized attempt at accessing the digital content data occurs" and "in the event of unauthorized access, reading a saturation profile of the system and system settings and generating saturation traffic on the system to deter unauthorized activity", as claimed in independent claim 126.

Since none of Reitmeier, *et al.*, Weidong, Jensen, *et al.*, Xu, *et al.* teach or suggest the limitations of independent claims 1, 29 and 89, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 1 and 89 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Weidong, and allowance of the claims, are respectfully requested. With regard to the

dependent claims 2-5, 11-14, 20, 25, 26, 90-92, 98-101, 107, 111 and 112, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 15-19, 21-24, 102-106 and 108-110 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Wiedong and Jensen, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 27, 28, 113 and 114 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Weidong and Xu, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend. Reconsideration of the rejection of independent claim 29 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 30, 32-39 and 43-53, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 40, 41 and 42 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Weidong, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 54 and 55 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Xu, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Further, since none of Reitmeier, *et al.*, Weidong and Jensen, *et al.* teach or suggest the limitations of independent claim 115, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claim 115 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Jensen, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 116, 118-121 and 123-125, it follows that these claims should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claim 122 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Jensen, *et al.* and Weidong, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Further, since none of Reitmeier, *et al.*, Jensen, *et al.* and Xu, *et al.* teach or suggest the limitations of independent claims 167 and 175, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 167 and 175 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Xu, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 168-171 and 176, it follows that this claim should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 172-174 and 177-179 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Jensen, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Further, since neither of Reitmeier, *et al.* and Jensen, *et al.* teaches or suggests the limitations of independent claims 85, 155, 161 and 180, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 85, 155, 161 and 180 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Jensen, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 86-87, 156-157, 162-166 and 181-183, it follows that this claim should inherit the allowability of the independent claims from which they depend.

Further, since none of Reitmeier, *et al.*, Xu, *et al.* and Atallah, *et al.* teaches or suggests the limitations of independent claims 56 and 126, there is no combination of the references that would teach or suggest these limitations. Accordingly, reconsideration of the rejection of independent claims 56 and 126 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* and Xu, *et al.*, and allowance of the claims, are respectfully requested. With regard to the dependent claims 57, 59-63, 127, 129, 130, 132 and 133, it follows that this claim should inherit the allowability of the independent claims from which they depend. With regard to the rejections of dependent claims 131 and 61 under 35 U.S.C. 103(a) as being unpatentable over Reitmeier, *et al.* in view of Xu, *et al.* and Atallah, *et al.*, it follows that these claims should inherit the allowability of the independent claims from which they depend.

Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

Authorization is hereby given to charge Deposit Account No. 50-1798 for any additional fees which may be due or to credit any overpayment.

Respectfully submitted,

Date: June 7, 2007

MILLS & ONELLO LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900
Facsimile: (617) 742-7774

J:\ECD\0012\amendmentb3.wpd

Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant